# MIPv6 Route Optimization Evaluation and Its Effects on Video Traffic in IPv6 Network

MINT 709 Capstone Project Report

April 2014

HIRAK PATEL

MSc Internetworking

Supervisor: Arsh Saini

# TABLE OF CONTENTS

# LIST OF FIGURES AND TABLES

## ABSTRACT

There has been a great deal of advancement in the field of technology in past 30 years. People are more connected than ever. Now personal computer is not the primary device to access the Internet, people are using smart phone and tablets for online shopping, watching movies and many more activities. Statistics shows that more than 40% of the Internet traffic is now coming from mobile users. According to Cisco VNI Mobile, video traffic for mobile was 53 percent of total traffic by the end of 2013.

IP is the dominant networking protocols in the Internet. Mobility support in IP is one of the many important subject area for research community all around the world. Mobile IPv4 (MIPv4) and Mobile IPv6 (MIPv6) are two protocols designed by IETF to support seamless mobility. MIPv6 is the next generation protocol that supports mobility in network layer. MIPv6 tries to overcome inherent flows of MIPv4.

The main goal of this project is to present performance analysis of Mobile IPv6. We will be using OMNeT++ in this project. On top of that we will be using INET Framework.

# 1 INTRODUCTION

In this technological advanced world, most of the Internet traffic and communication is mobile. This means that during operation they need to move around various networks with different network prefixes (subnets). Most of the Internet technologies use IP as networking protocol for fixed and mobile networks. Initially IP was provisioned for only end to end connectivity between hosts that had a fixed point of attachment. IP addresses are used for identifying network that host belong to and that host in network itself. This is not ideal for mobile routing. Because you need stable IP address to identify host but if you have stable IP address for host then if that host move around in different subnet changing its point of attachment, packet destined to that host will get lost. There are several approaches that supports mobility on the Internet. Mobile IP was designed by Internet Engineering Task Force (IETF) to support mobility at network layer. The Mobile IP protocol ensures seamless session connectivity in almost all circumstances. It means the ability to not lose connection on application-level while changing point of attachment as mobile devices move around on the Internet.

The next generation of protocol that support mobility on network layer is Mobile IPv6 (MIPv6). The development of Mobile IPv6 benefits from the development of Mobile IP support in IPv4 (MIPv4) and extensive features of IPv6. Although Mobile IPv6 has many advantages over Mobile IPv4, it is not widely used due to several technical difficulties. To overcome these problems many protocols have been proposed that tries to enhance performance and functionality.

Next generation networks are expected to support real time multimedia application with high payload and with highly time sensitive data. End to end delay is a parameter that must be kept under certain threshold value. Therefore, the main issues in network mobility is Route optimization. Route optimization techniques are required to handle end to end delay. Many route optimization techniques have been proposed up till now.

Main goal of this project is to study Mobile IPv6 (MIPv6) Route Optimization mechanism and evaluate the effects of MIPv6 Route Optimization mechanism for real time application like video traffic in proposed IPv6 environment in OMNeT++ simulator.

# 2 LITERATURE OVERVIEW

The widespread development of mobile technologies require extensive support at network layer. It was necessary to develop such technology that supports seamless user mobility while Mobile nodes change their point of attachment on the Internet. The following properties should be taken into account to support mobility of nodes:

**Handover**: Handover refers to the process of transferring ongoing session from one network to another network. The performance of mobility scheme mainly depends on the type of handover it uses. There are two types of handover mechanisms: Soft and Hard Handover. Soft handover tries to make new connection before disconnecting the previous connection. In soft handover, Mobile nodes can communicate with multiple interface and communication with old interface is cut down when signal strength with old access point dropped below certain threshold value. Hard handover drop previous connection before making new one. Handover should be handled efficiently to reduce end to end delay or even loss of packets.

**Quality of Service (Qos):** Quality of service should not be depreciated when handover takes place in mobile network.

**Transparency:** The mobility scheme should be transparent to applications. It means that when handover happens it should be transparent to the application and application should work fine without restarting it.

**Scalability:** The mobility scheme is said to be scalable if its performance does not diminish as number of MNs (Mobile Node) and CNs (Correspondent Node) increases.

**Fault Tolerance:** The mobility scheme should be fault tolerant. It means that it should work in presence of failure. A mobility scheme should make the communication between mobile nodes as much tolerant to fault as the communication between stationary nodes.

**Routing:** The mobility scheme should be designed in such manner that packets should be routed with as low latency as possible.

**Security:** Security is a crucial issue in a wireless environment. Mobility management schemes should not introduce additional security issues to the network. Also, the interruption of connectivity due to the time required for authentication process should be avoided.

**Location Management:** If a mobile host offers services to other nodes, it must be located by these nodes as it moves, as well as keeping the privacy of its topological location.

**Link layer independence:** User should be able to seamlessly operate across heterogeneous link layer technologies, not all of which support the same link layer mobility scheme.

First we will look into different categories of mobility.

Host Mobility refers to an end node changing its point of attachment without any interruption between host and correspondent Node. Network Mobility refers to Mobile IP subnet changing its point of attachment to an IP backbone.

In IP Mobile Multicasting, instead of sending data to a single node, multicasting delivers data to a set of selected receivers. In IP multicast, a source sends a single copy of a packet and the network duplicates the packet as needed until the packet reaches all the selected receivers. This avoids the overhead associated with both replication of packets at the source and sending duplicated packets over the same link.

“Micro” and “Macro” are often used to refer to the scale of mobility. Micro-mobility tends to deal with situations where a subscriber is seamlessly moving between two points of attachment that are part of the same network. Macro-mobility tends to deal with situations where a subscriber is seamlessly moving between networks (regardless of operational control). Many well-known proposals have been developed to support macro-mobility. Mobile IP is one of the many solution that handles macro-mobility problem. Mobile IP is well suited for macro-mobility due to their mechanisms for achieving efficient handoff, packet loss, efficient routing of packets, etc.

In the following section we will try to provide background description on protocols that currently support mobility at Network layer: Mobile IPv4 (MIPv4), Mobile IPv6 (MIPv6). After that we will be comparing Mobile IPv4 with Mobile IPv6. Then detailed explanation on Route optimization in Mobile IPv6.

## 2.1 MOBILE IPV4

Mobile IP is the first approach towards solving mobility problem at Network Layer. Mobile IP version 4 is designed to allow mobile devices to change their point of attachment on internet while maintaining the same IP address. Mobile IP according to its formal definition is the standard that allows users using Mobile devices whose IP is associated to one network to stay connected when moving to other networks. It is developed by Internet Engineering Task Force and is described in IETF RFC-5944. Mobile IP seemed to solve many issues related to Mobility. It provides transparency, and we do not have to change application behavior in order to support mobility. Mobile IP is intended to enable nodes to move from one subnet to another. Mobile IP facilitates node movement from one Ethernet segment to another and to wireless LAN as well, as long as the Mobile Node's IP address remains the same after such a movement. Mobile IP is scalable as it is built on top of IP. Mobile IP enhance IP functionality to have two IP addresses for Mobile Nodes, first one is for permanent Identifier which is Home Address and other is for Routing IP datagrams and called as Care-of Address. Main goal of the Mobile IP is to maintain the TCP connection between mobile host and static host across the network while reducing the effects of location changes while mobile host is moving around without having to change underlying protocol stack. Mobile IP was designed to support seamless and continuous internet connectivity.

The Mobile IP protocol allows location-independent routing of IP datagrams on Internet. Each Mobile host is identified by its Home Address which is permanent regardless of its location on the Internet. While moving away from Home network, mobile node is associated with another IP address known as care-of Address which is useful in identifying Mobile Node's current location in foreign network.

To understand Mobile IP we need to understand following terminologies first:

**Mobile Node:** An end host that changes its point of attachment from one network to another.

**Home Network:** Network which mobile node was associated with before moving to a new network. In other terms a network that has prefix matching that of Mobile Node's home address. Hence IP datagrams which are destined for Mobile node will be delivered to Mobile Node's Home Network.

**Foreign Network:** Any network that is not mobile node's home network.

**Home Address (HoA):** A permanent IP assigned to mobile node regardless of its location on the Internet. It is also the IP address of Mobile node in its original network (Home Network).

**Home Agent:** Home Agent is a router on a home network of mobile node. It will tunnels datagram for delivery to mobile node while away from the home network and maintains the information about current location of Mobile Node.

**Foreign Agent:** A router on foreign network that cooperates with home agent in order to route datagrams to mobile node while it is visiting foreign network. It will deliver datagrams to mobile node, datagrams that were tunneled by the Mobile Node's Home agent. And for datagrams that are sent by mobile node, foreign agent will act as default router on foreign network.

**Care-of Address (CoA):** Care-of address is a temporary IP address for a mobile node that enables datagram delivery when mobile node is in foreign network. Mobile IP registers its Care-of address to home agent. So when a datagram for Mobile node delivered to Home network while mobile node is in foreign network, home agent intercepts the message and tunnels it back to mobile node's CoA.

**Correspondent Node:** Any node (host) with which mobile node is communicating. That node is may be fixed or mobile.

**Mobility Binding:** The association of a Home address with care-of address.

### 2.1.1 Overview

In this section a brief description is given of Mobile IP's operation:

**Agent Discovery:** Home and Foreign Agents advertise their presence on each link on which they operate. Mobile node will send solicitation message to learn agent's presence.

**Registration:** The method of registering care-of address to home agent when mobile node is away from home network. Depending on Mobile node's method of attachment, mobile node registers directly to home agent or via foreign agent which will forward the registration to home agent.

First, both agents (Home & Foreign) will advertise their presence via Agent Advertisement message. MN listens for agent advertisement message in order to determine whether it is in home network or foreign network and to bind with home agent or foreign agent. MN can also send agent solicitation messages to trigger mobile agents.

And when MN detects that it is in its home network, it will be configured with its home address. It operates without mobility services. When MN detects that it is away from home network in any foreign network it attains care-of address (CoA). MN can get CoA from foreign agent by foreign agent's advertisement that is foreign agent care-of address or some external method such as using DHCP (co-located care-of address). Foreign agent CoA is preferred because other MNs can use the same address and therefore does not place unnecessary demands on already limited IPv4 address space. In case of co-located CoA unique address is assigned to every MN. In case of foreign agent CoA, FA is endpoint of the tunnel that is between HA and FA when MN is in foreign network. So when FA receives tunneled datagrams it will decapsulates them and deliver decapsulated datagram to MN. In case of co-located CoA, MN is endpoint of tunnel and itself performs decapsulation on datagrams that are meant for MN. The advantage of using co-located address over foreign agent CoA is that it allows MN to work without FA. Although it has drawback of using unique IP address for each MN hence placing burden on IPv4 address space.

Then MN that is away from home will registers its newly assigned CoA to home agent through exchange of Registration request and Registration reply messages. MN can do this either through FA or directly in case of co-located CoA and there is no necessity to use FA.

When HA receives registration request from MN, it validates the message and see if MN’s home address is in same subnet. If registration request is valid HA will set up a tunnel with the CoA and sets up mobility binding with CoA. HA sends binding acknowledgement to MN through FA or directly to MN. After that datagrams that are sent to MN will be intercepted by MN’s HA and tunneled to MN’s CoA. The tunnel endpoint can be either FA or MN. MN uses home address to send datagrams to correspondent node all the time, hence creating transparent mobility to CN. In foreign network MN can send datagrams to CN either directly or through home agent. It can use its permanent home address as source address for the IP datagrams. This mode of routing is known as Triangular Routing or “Route Optimization” mode. In other method, sending datagram via Home agent is called *reverse tunneling.* Here Home agent in turn will forward packet to correspondent node. Reverse tunneling is needed in networks whose gateway router check the source IP address of the packet to see if it belongs to their subnet or discard it otherwise.   Advantage of using tunnel is that intervening routers between HA and FA will not have knowledge of Mobile Node’s Home Address.

When using co-located care-of address, MN must be located on the link identified by CoA network prefix. Else datagrams destined to CoA will be dropped (Undeliverable).

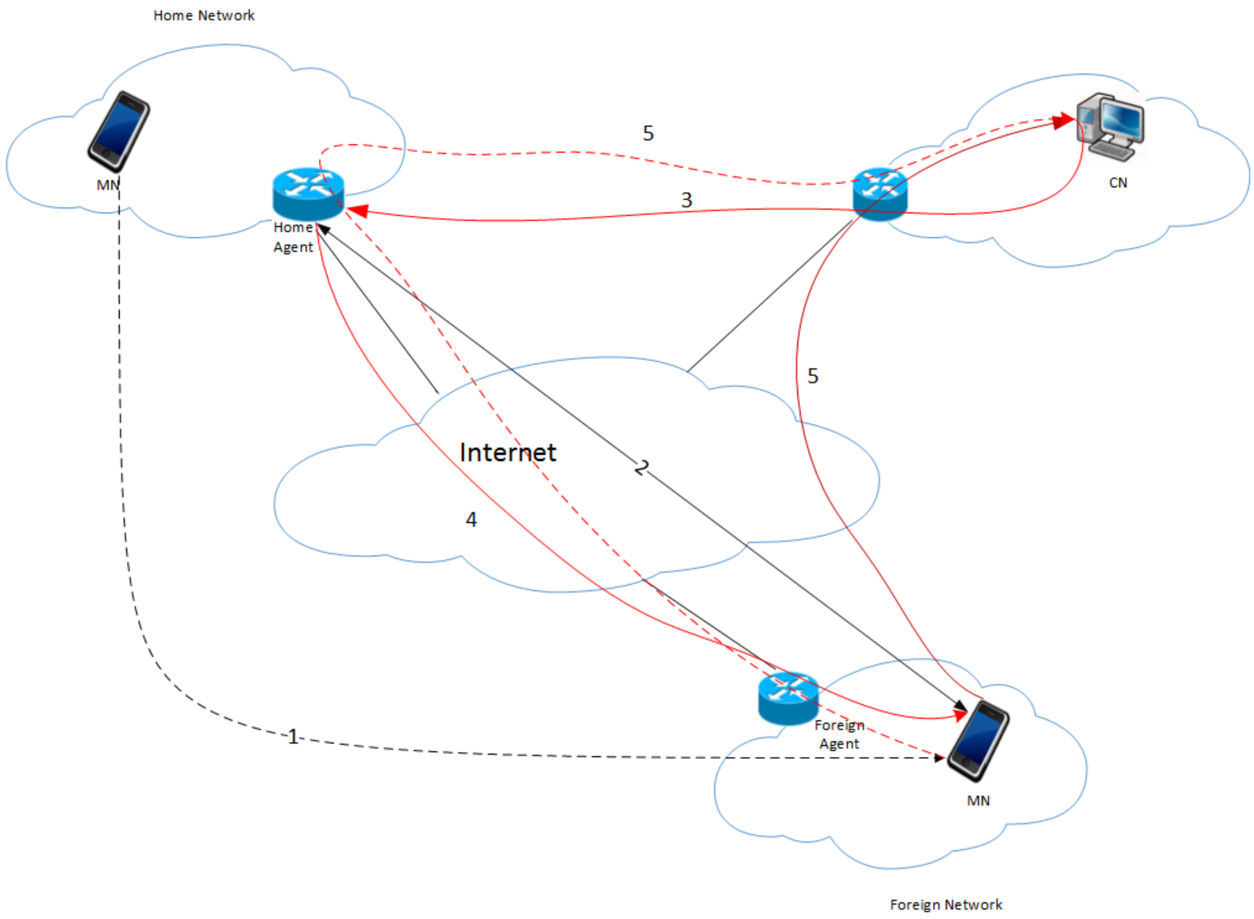

*Figure 1: MIPv4*

As shown in figure:

(1) The mobile node move away from Home Network and goes to Foreign Network and gets new Care-of Address.

(2) Through newly acquired CoA MN will send Binding Update to Home Agent. HA will send Binding Acknowledgement to MN.

(3) CN is sending data to MN, HA will intercept the datagrams destined to MN's Home Address.

(4) Then HA tunnels datagrams destined to MN from CN using MN's care-of Address.

(5) When MN wants to send data to CN, it can send data directly to CN or it can tunnel all datagram through HA.

## 2.2 MOBILE IPV6

IPv6 is the next generation protocol for the network layer. It is developed by the Internet Engineering Task Force to resolve the IPv4 address exhaustion problem. IPv6 is intended to replace IPv4 which is widely used. But with the increasing number of devices on the Internet we need larger address space. At the moment IPv4 provides $2^{32}$ addresses. IPv6 provide $2^{128}$ addresses, more than 7.9 x $10^{28}$ times as many as IPv4. IPv6 protocol have several advantages over IPv4. Some of them are:

- Larger address space
- Security (Built in authentication and privacy support)
- Improved support with Extension headers
- Better Performance
- Automatic address configuration
- Improved QoS with Flow-labelling
- Better Multicast Routing
- Simpler Header format

### 2.2.1 Neighbor Discovery Protocol

To understand Mobile IPv6 clearly we need to understand Neighbor Discovery Protocol that is used with IPv6. It works on Link-layer and it is responsible for address auto configuration of nodes in network, assigning link layer address to links, finding nodes on link, duplicate address detection, address prefix discovery and maintain reachability information to active nodes in network.

*Neighbor Discovery uses these addresses for its services:*

- **All-nodes multicast address**: link-local scope address to reach all nodes with prefix FF02::1.
- **All-routers multicast address:** link-local scope address to reach all routers with prefix FF02::2.
- **Solicited-node multicast address:** link-local scope with prefix FF02::1:FF00/104. Every IPv6 host should have at least one address per interface. A node is required to compute and join the associated Solicited-Node multicast addresses for all unicast and anycast addresses that have been configured for the node's interfaces.
- **Link-local address:** link-local unicast address with prefix FE80::/64. Used to reach neighbors. All interfaces on nodes must have a link-local address.

*Neighbor Discovery Protocol aims to provide following set of functionality:*

- **Prefix Discovery:** Hosts can discover address prefixes that are on link for attached links. Nodes uses prefixes to distinguish destination is on-link or off-link.
- **Router Discovery:** Hosts can discover routers that are attached on link.
- **Address Autoconfiguration:** Allow nodes to configure addresses for an interface in stateless manner.
- **Address resolution:** Hosts can determine link-layer address of an on-link destination by its IP address.
- **Duplicate address detection (DAD):** Hosts can determine whether an address is already in use or not.
- **Parameter discovery:** Hosts can find link parameters.
- **Next-hop determination:** Hosts can find next hop routers for specific destination.
- **Neighbor Unreachability Detection:** Hosts can determine whether neighbor is reachable or not.
- **Redirect:** Hosts can find better next-hop for particular destination.

*Now to serve all these functionality NDP uses following ICMPv6 messages:*

- **Router Solicitation:** When interface goes “UP”, host will send out Router Solicitation message to trigger routers to generate Router Advertisements rather than waiting for them at scheduled time.
- **Router Advertisement:** Router will send out this message periodically or in response to host’s router solicitation message. Router uses this message to advertise their presence on links.
- **Neighbor Solicitation:** Nodes uses this message to determine link-layer address of a neighbor and also to determine whether neighbor is reachable or not by cached link layer address. Also useful in Duplicate address detection.
- **Neighbor Advertisement:** Neighbor Advertisement messages are used by nodes to respond to Neighbor Solicitation messages. Nodes can also send unsolicited neighbor advertisement for link-layer address change.
- **Redirect:** Routers use this message to inform host about better first hop for particular destination.

#### *2.2.1.1 Prefix Discovery*

Generally hosts determine network prefixes from router advertisement messages. A network prefix is globally unique 64-bit value, usually consisting of 48-bit organizational prefix and followed by unique within organization 16-bit subnet ID. Another way hosts can obtain subnet prefix is from DHCPv6 using prefix delegation. A single Router Advertisement may have multiple prefix information options.

#### *2.2.1.2 Router Discovery*

Router will send out Router Advertisement messages either periodically or in response to host's router solicitation messages on multicast-capable links. Host will receive router advertisement message from all routers and build database for default routers. Router advertisement messages contains the information required by hosts to determine prefixes, MTU, specific routes, address validity, whether to use address autoconfiguration or not.

#### *2.2.1.3 Parameter Discovery*

Parameter Discovery works same way as Prefix Discovery by sending Router Solicitation message to all router on local link multicast address (ff02::2). In Router advertisement message desired information is in MTU option.

#### *2.2.1.4 Address Autoconfiguration*

Neighbor Discovery Protocol provides mechanism for host to automatically configure itself with an address learned through prefix discovery. This mechanism is stateless address autoconfiguration. Stateless address autoconfiguration enables host to create their address by combining the prefix advertised by local routers and interface identifiers (MAC address). In stateful address configuration, hosts use DHCPv6 to acquire address information.

#### *2.2.1.5 Address Resolution*

Address resolution is used to map IPv6 address to link-layer address. In IPv4 this can be done by ARP. Here host seeking the link layer address of a neighbor multicasts neighbor solicitation message and the neighbor responds with its link layer address in Neighbor Advertisement.

#### *2.2.1.6 Duplicate Address Detection*

This mechanism is used to determine if a tentative address is already in use by other node on local link. Nodes (Host and Router) perform DAD on all unicast addresses. In IPv4 DAD is performed by gratuitous ARP request. Node with the tentative address sends Neighbor Solicitation message with source address as unspecified address (::) and destination address is the solicited node multicast address for the tentative address. Target address is the tentative address itself. If any other node is using that address it will respond with Neighbor Advertisement message. If host does not receive any neighbor advertisement message in specific timeout interval then host is allowed to use that address.

#### *2.2.1.7 Next-hop Determination*

To send datagrams to other nodes, sending node first must determine if destination is on-link or off-link. If it is on-link the next-hop address is the destination address. And if it is off-link then the next-hop address is the default gateway of the sending node.

#### *2.2.1.8 Neighbor Unreachability Detection*

Nodes can check neighbor reachability by sending neighbor solicitation message and wait for neighbor advertisement message from that neighbor. If not received in certain time period, node will delete neighbor cache entry.

#### *2.2.1.9 Redirect*

Redirect is used by router to tell sender node that more preferable route is available. This message can also be used by default gateway node to inform an internal node (that is sending datagram) that destination is on-link not off-link.

### 2.2.2 Mobile IPv6 Operation

Mobile IPv6 is designed using IPv6 features mentioned above. Mobile IPv6 is developed by Internet Engineering Task Force that supports mobility in IPv6 networks. MIPv6 standard is described in detail in RFC-3775. The need for Mobile IPv6 was necessary because in the IPv6 network if node is moving from one network to another then it cannot maintain the address that is assigned to it previously, hence unreachable. So, Mobile IPv6 allows mobile node to move from one subnet to another without changing its address that is called “Home Address”. Datagrams that are destined to mobile node can be routed using this home address regardless of its current point of attachment on the Internet. The movement of mobile node is transparent to higher-layer protocols and applications. Mobile IPv6 solves many network management problems. For example handover among wireless transceivers have been resolved by using link-layer techniques. But Mobile IPv6 does not attempt to solve all problems related to mobility.

There are several terms we need to understand first to comprehend MIPv6 more clearly.

- **Mobile Node:** A node that changes its point of attachment on internet while still reachable by its home address.
- **Home Address:** A unicast routable address assigned to MN. It is used as permanent address of MN. Mobile Nodes can have multiple home addresses when there are multiple home prefixes on home link.
- **Home subnet prefix:** The subnet prefixes which corresponds to MN’s home address.
- **Home link:** The link on which Mobile node’s home subnet prefix is defined.
- **L2 Handover:** Process in which mobile node changes its link layer connection. Change of wireless access point is L2 Handover.
- **L3 Handover:** L3 handover happens when mobile node detects a change in an on-link subnet prefix that would require a change in care-of address. Change of access router involves L3 handover.
- **Foreign subnet prefix:** Any subnet prefix other than home subnet prefix.
- **Foreign link:** Any link other than mobile node’s home link.
- **Care-of Address:** A unicast routable address associated with MN while visiting a foreign link, subnet prefix of CoA is foreign subnet prefix. There can be more than one CoA associated with one mobile node. But the one which is registered with mobile node’s home agent for a given home address is called its “primary” care-of address.
- **Binding:** Association of care-of address with home address for that mobile node along with the remaining lifetime of that association.

- **Registration:** Mobile node sends Binding Update to home agent or correspondent node causing binding for the mobile node to be registered.
- **Return routability procedure:** This procedure authorizes registrations by the use of cryptographic token exchange.
- **Cookie:** A cookie is a random number used by mobile node to avoid connection from fake CN in return routability procedure.
- **Binding Cache (BC):** This usually maintained by home agents and CNs. It is useful in route optimization. Binding cache contains home address of MN for which this is BC entry, CoA of MN indicated by home address field in BC entry, lifetime value indicating validity for this BC entry.
- **Binding Update List (BUL):** This list is maintained by MN. BUL records information of each binding update sent by MN with valid lifetime. It contains all the bindings sent by MN either to its home agent or CN. It also contains the binding updates that are waiting for return routability procedure. Among multiple binding updates that are sent to the same destination, most recent one is kept in BUL.
- **Home Agents List (HAL):** This list is maintained by HA. HAL contains information about routers that are acting as home agent on the same link. HAL is used by dynamic home agent discovery mechanism.

Using Mobility header MIPv6 defines some new messages that are used in the protocol:

- **Home Test Init, Home Test, Care-of Test Init, and Care-of Test:** These messages are used for return routability procedure from MN to CN
- **Binding Update:** Used by MN to acknowledge HA or CN of its current binding.
- **Binding Ack:** Used to acknowledge the receipt of a BU.
- **Binding Refresh Request:** Used by CN to request MN to refresh its binding with CN.
- **Binding Error:** Used by CN to generate an error related to mobility.

Mobile IPv6 introduces new IPv6 destination option by IPv6 Destination option extension header. Used by MN in foreign network to inform CN about MN's home address.

Mobile IPv6 uses four new ICMP messages. Two of them are used for dynamic home agent discovery mechanism and another two are for network renumbering and mobile configuration mechanisms. For Dynamic Home Agent Discovery Mechanism, "Home Agent Address Discovery Request" and "Home Agent Address Discovery Reply" messages are used, and for renumbering and mobile address configuration "Mobile Prefix Solicitation" and "Mobile Prefix Advertisement" messages are used.

Mobile node is always expected to be reachable at its home address irrespective of its location on the internet. If Mobile node is at home network than datagrams addressed to its home address will be delivered through conventional routing mechanisms. And, when mobile node is in foreign network it can be reached through one or more care-of addresses. Care-of address can be acquired through stateless or stateful address autoconfiguration. So in foreign network mobile node can be reached through this care-of address. Mobile node can have several care-of addresses but at a time only one “primary care-of address” will be used in binding process. While away from home network MN registers its primary care-of address with a router on its home link, requesting this router to function as “Home Agent” for the mobile node. Mobile Node will perform this binding registration by sending a “Binding Update” message to home agent. Home Agent acknowledges this registration request with “Binding Acknowledgement” message and makes an association between the home address of mobile node and the care-of address it receives.

Correspondent Node can be identified as any node in network that is communicating with Mobile Node. It can be either stationary or mobile. Mobile Nodes usually provide information about their current location to correspondent nodes. This information can be provided through correspondent registration. It means “Binding” between Mobile Node and Correspondent node. But before this binding, Return Routability Test is performed to authorize the establishment of the binding.

*There are two possible modes for communication between the mobile node and correspondent node:*

**Bidirectional Tunneling:** This mode of communication does not require Mobile IPv6 support from the CN. In this mode, mobile node does not register binding with the correspondent node. If correspondent node is sending data to mobile node then packets will be routed to the home agent first and then tunneled to mobile node. And packets from mobile node to correspondent node first tunneled from mobile node to home agent and then home agent to correspondent node. In bidirectional tunneling home agents uses proxy Neighbor Discovery mechanism to intercept packets destined to mobile node’s home address on home link, then these packets are tunneled to the mobile node’s primary care-of address. Tunneling is performed using IPv6 encapsulation.

Steps:

(1) Mobile Node leaves home network and goes into foreign network.
(2) MN sends Binding Update message to its home agent containing IPv6 Destination option (Home Address Option) that has MN’s home address.
(3) Home Agent validates the binding update message. It will associate care-of address from source address to home address and creates a binding cache entry. After this it will send binding acknowledgement to mobile node confirming the association. In Binding Acknowledgement message destination address is MN’s care-of address but it contains IPv6 Routing Header option that has MN’s home address.
Mobile node will validate Binding Acknowledgement and if it is valid than mobile node adds a Binding Update List entry or update if there was a previous entry and informs other nodes in BUL about the update by sending them BU message.

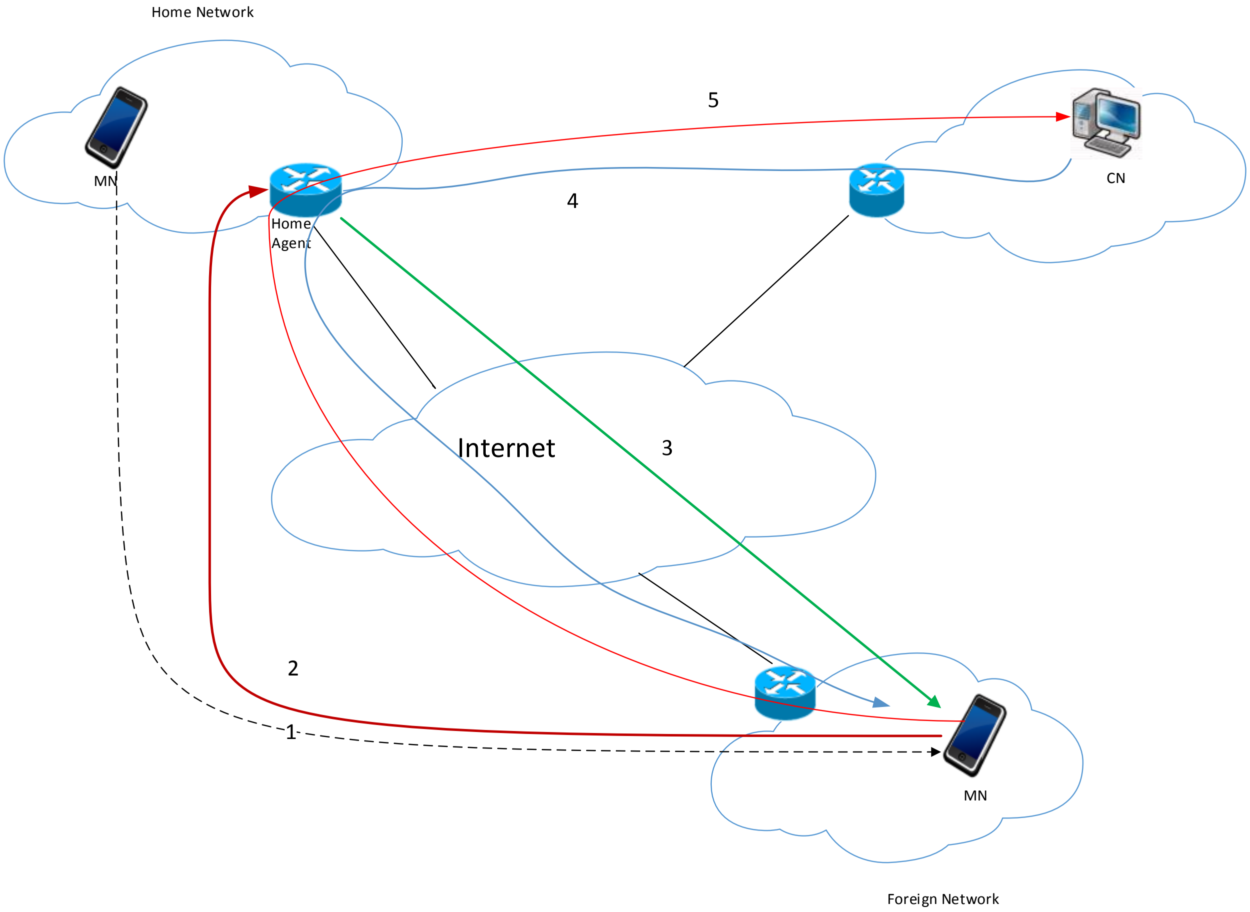

*Figure 2: Bidirectional Tunneling*

(4) Packets going from mobile node to correspondent node will intercepted by home agent first and then tunneled to correspondent node. Here packets that are being intercepted at home agent have source address as CoA of mobile node. They also contains IPv6 destination option (Home Address Option) that have MN's home address.

(5) Packets going from correspondent node to mobile node also will be intercepted by home agent and then tunneled to mobile node. Here packets will have MN's CoA as destination address and MN's home address in routing header option.

**Route Optimization:** This mode of communication requires mobile node to register its current binding at the correspondent node. Usually mobile node use home address as the source address of the packets it sends to correspondent nodes except in some short term communication it uses care-of address. If mobile node uses home address as its source address then it will be tunneled to home agent first and then to correspondent node with outer source address as mobile node's care-of address. This approach presents the same problem as in MIPv4 of Triangular Routing. Route optimization solves this problem. But for that correspondent node must have support for route optimization. Following requirements apply to all CN's that support route optimization:

- CN must be able to validate Home Address option using an existing Binding Cache entry
- CN must be able to insert type 2 routing header into outbound packets to mobile node
- CN must be able to ignore packets with type 2 routing header. It must silently discard packets that it has received with such headers
- CN must be able to process mobility headers
- CN must be able to participate in a return routability procedure
- CN must be able to process binding update and acknowledgement messages
- CN should allow route optimization to be administratively manageable

When MN receives first packet from CN that it has not a binding with, it will start return routability procedure. Return Routability procedure starts by sending two messages to correspondent node, one directly Care-of Test Init (CoTI) and one through home agent Home Test Init (HoTI). HoTI message will be validate by home agent. CN replies back with Care-of Test (CoT) and Home Test (HoT) messages. Upon receiving these messages and using information from these messages MN sends a Binding Update to correspondent node. CN validates BU and adds entry into binding cache and sends binding acknowledgement. MN receives BA and check if it is valid or invalid, if it is valid MN will add an entry to its BUL. Now packets from correspondent node can be directly routed to MN's CoA. Routing packets directly to MN's CoA allows the shortest communication path to be used. It also eliminates congestion at the MN's home agent.

Packets going to MN from CN can be directly routed to mobile node, CN uses care-of address of mobile node as destination address in IPv6 header. In that IPv6 packet type-2 routing header option including MN's HoA is also used. Similarly MN uses its care-of address as the source address in packet's IPv6 header and uses home address destination option to carry its home address. The inclusion of home address in these packets makes the use of care-of address transparent at the transport layer.

When Binding lifetime is about to expire CN sends Binding Refresh Request to the Mobile Node. And Mobile Node responds with Binding Update message. CN can send Binding Error message to mobile node in response to Binding Update message if it does not have Binding Cache entry for mobile node.

Return Routability procedure plays an important role in route optimization of Mobile IPv6. The advantage of the return routability procedure is that it is lightweight and does not depend on a public-key infrastructure or on pre-existing relationship between MN & CN. This is very important in broad deployment. On contrary, this process has an adverse impact on handover delays and results in longer handover delay and increased overhead as it involves signaling among all the three nodes MN, HA, and CN involved in the mobility management. Because messages that are used in procedure consist of end to end message exchange between mobile node and correspondent node. Home Address Test message has higher impact as it routes through home agent. Return Routability procedure is also exposed to attackers that are in position where they can interfere in home and care-of address test. It can be limited by repeating return routability procedure every 7 minutes. But this will increase signaling overhead. Return routability procedure protects binding updates against all attackers who are unable to monitor the path between the home agent and correspondent node. The procedure does not defend against who can monitor this path. To overcome these drawbacks IETF has developed Enhanced Route Optimization. It is described in RFC 4866.

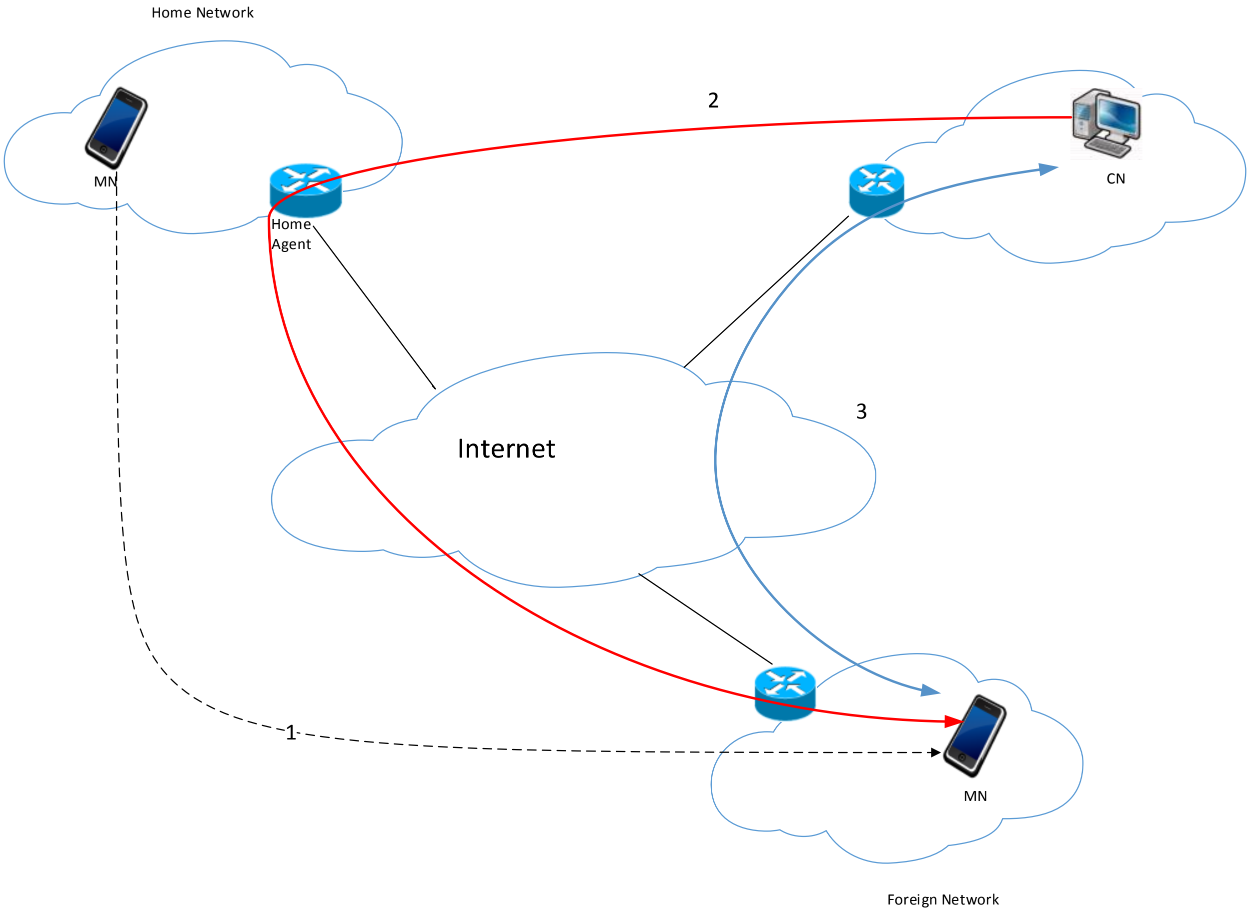

*Figure 3: Route Optimization*

Steps:

(1) Mobile Node leaves home network and goes into foreign network.
(2) MN receives first packet and starts return routability procedure.
(3) Now MN and send can directly communicate with each other.

### 2.2.3 Enhanced Route Optimization for MIPv6

MIPv6 route optimization enables mobile and correspondent node to communicate directly. The association between home address and care-of address of the mobile node is called Binding. It is the responsibility of mobile node to update its binding to CN through “correspondent registration” when it changes IP connectivity. Mobile node keeps home agent up to date about its whereabouts and its current care-of address by “home registrations”. From a security perspective, establishment of binding during correspondent registration requires CN to verify MN’s association of home address and care-of address. For this purpose return routability procedure is used. Messages that are used in return routability procedure ensures the reachability to MN’s home address and care-of address.

Enhanced Route Optimization for MIPv6 uses cryptographically generated addresses to improve security and reduce handover delays. It uses public/private key pair to secure addresses. It secures mobile node’s home address against impersonation through an interface identifier that is public component of the mobile node’s public/private key pair. Mobile node attests its identity by providing corresponding private key. It allows a mobile node to authenticate to a correspondent node based on the CGA-cryptographically generated address property of its home address. Enhanced Route Optimization enables correspondent registration in parallel with the respective home registration for mobile node.  This reduces handoff delays compared to base Mobile IPv6 route optimization, which requires mobile nodes to wait for a binding acknowledgment message signifying a successful home registration before they start a correspondent registration. The use of cryptographically generated home addresses reduces threat of interpose that can interpose on home address test and therefore longer binding lifetimes. This helps in increased security and reduction in signaling overhead. Cryptographically generated home addresses and concurrent care-of address tests are preferably applied together.

Using CGA in enhanced route optimization may increase computational cost as the use of CGA requires computationally expensive algorithms. This may be issue for small mobile devices with low processing power. It creates problem for correspondent node that is communicating with many mobile nodes simultaneously. The correspondent node have to secure itself from denial of service attacks by limiting the amount of resources it spends on CGA.

### 2.2.4 Security Considerations in MIPv6

In Mobile IPv6 most of the potential security threats are related to false bindings that usually results in denial of service attacks.

Some of the threats are:

- Man-in-the-middle, Hijacking, Confidentiality and Impersonation attacks.
- Authentication of binding messages to home agent. An attacker send wrong binding update and mobile node might not get traffic destined to it and attacker intercepts that traffic.
- Threats against route optimization on correspondent node. An attacker will send binding update to correspondent node with home address set to attacker's address rather than mobile node's home address. If correspondent node accepts this binding update then communication between mobile node and correspondent node is disturbed and data from correspondent node is sent to attacker's address. In this situation attacker will be successful in redirecting packets destined to mobile node to itself. This is threat to confidentiality and availability.

  An attacker may also send large number of binding updates to correspondent node. These binding updates will occupy CN's resources to check its validity causing denial of service attack.
- Threats on tunnel between mobile node and home agent while impersonating as mobile node
- Threats on using type-2 routing header to find a way around firewall.
- Threats against security mechanism that has been deployed in MIPv6. Forcing these mechanisms to use cryptographic computationally expensive algorithms.

MIPv6 relies on IPv6 features to provide security, Internet Protocol Security Architecture (IPSec) provides necessary mechanisms for authentication and encryption. MIPv6 protocol specifies that all packets carrying Binding Update and Binding Acknowledgement destination options must be authenticated using Authentication Header or Encapsulating Security Payload Header. These headers provide sender authentication, data integrity protection and communication privacy protection.

IPSec used to authenticate and encrypt packets. It was the first proposed solution to authenticate binding messages. The biggest problem with IPSec is key distribution. Key distribution is also known as Internet Key Exchange. It uses pre-shared secret or private keys in the key exchange. Return Routability Procedure is also used to provide adequate authentication between mobile node and correspondent node.

## 2.3 COMPARISON BETWEEN MIPV4 AND MIPV6

Mobile IPv6 benefits from experience gained from Mobile IPv4 development and from the features provided by IPv6. Thus, Mobile IPv6 and Mobile IPv4 have many major similar functionalities but MIPv6 offers many improvements. This section summarizes the major difference between Mobile IPv4 and Mobile IPv6:

- There is no need for foreign agent in Mobile IPv6 as it relies on DHCPv6 or stateless address autoconfiguration on the foreign network to acquire care-of address. So this makes it easier for mobile node to operate in any location on the Internet without requiring additional support from router on foreign network. Mobile IPv4 does not have this support so it needs foreign agent to operate in foreign network.
- Support for Route Optimization is fundamental part of the protocol rather than a nonstandard part of the extension. For efficient route optimization routers that support "ingress filtering" are used in Mobile IPv6.
- Mobile IPv6 route optimization can operate securely with the help of return routability procedure and it does not require any pre-arranged security associations. It can be deployed on global scale between all mobile nodes and correspondent nodes.
- The dynamic home agent discovery mechanism in Mobile IPv6 is more efficient than directed broadcast approach used in Mobile IPv4. Because dynamic home agent discovery mechanism returns a single reply to mobile node and direct broadcast approach returns separate replies from each home agent.
- Mobile IPv6 is more robust then Mobile IPv4 as it is decoupled from particular link layer because it uses IPv6 Neighbor Discovery instead of ARP.
- The use of type-2 routing header (extension header of IPv6) reduces the overhead compared to Mobile IPv4. While away from home mobile ipv6 uses routing header rather than IP encapsulation in MIPv4 to send datagrams to mobile node.
- IPv6 Neighbor Unreachability Detection ensures reachability between mobile node and its service router in the current location.

# 3 NETWORK MODEL AND IMPLEMENTATION

This chapter describes simulation setup for the proposed network in OMNeT++. Brief introduction about OMNeT++ and its components. Introduction about framework that is used to support the proposed network model and different components that are being used in it.

## 3.1 SIMULATION FRAMEWORK

For this project, simulation is carried out in OMNeT++ tool. OMNeT++ is an object-oriented modular discrete event network simulation framework.  OMNeT++ has fully object-oriented architecture. Network models can be formed by combining other modules that are either simple modules or compound modules. Simple modules are written in C++ using the simulation class library and they encapsulate model behavior. Compound module consists of many simple modules. Well-written modules are reusable. Modules communicate via message passing. They can pass messages via gates and connections that are predefined. The depth of module nesting is unlimited, you can combine as many simple or compound module to make model. OMNeT++ model are often referred as Network. Model structure is defined in Network Description language (NED language). To support the simulation there is one configuration file provided in that we assign value to parameters. Parameters are used to customize the network behavior. You can pass string, integer or Boolean values to parameter. You can pass XML data structure to parameters as well.

OMNeT++ provides basic framework and tools to write simulations but it does not provide any specific components for computer network simulations. External frameworks and simulation models are developed to support these simulations. OMNeT++ simulations can be run under various user interfaces. This can be really helpful in demonstrating and debugging purposes. OMNeT++ is free only for academic and non-profit use.

For this project we used OMNeT++ 4.3.1 version. We also used xMIPv6 simulation model to support our simulation that is based on INET framework.

### 3.1.1 INET Framework

The INET Framework is an open-source communication networks simulation package for OMNeT++. The INET Framework provides support for several wired and wireless networking protocols. INET Framework contains IPv4, IPv6, TCP, UDP, SCTP protocol implementations and many other application models. It also has MPLS support for IPv4 with RSVP-TE and LDP signaling. It also provide support for Link-layer with implementations of Ethernet, PPP and

802.11. Routing can be setup using either autoconfigurators or routing protocol implementations. INET Framework provide support for mobile simulations as well.

### 3.1.2 xMIPv6

xMIPv6 is simulation model that has been developed in accordance with IETF‘s official specification for Mobile IPv6 protocol that has been standardized in RFC 3775. There has been efforts to develop simulation model for MIPv6 in past like IPv6SuiteWithINET developed in 2004. This implementation was developed as an independent framework and hence it does not scale well to new developments in INET Framework. The xMIPv6 simulation model was developed conforming to the basic design and coding style of the official INET Framework. The xMIPv6 simulation model was developed with minimal modifications to other modules such as IPv6, IPv6NeighborDiscovery, RoutingTable6, InterfaceEntry, InterfaceTable, IPv6InterfaceData etc. without modifying base INET Framework functionality.

Following operations are supported by xMIPv6 simulation model:

- Generic movement detection
- Stateless address auto-configuration
- CoA auto-configuration
- Home registration
- Reverse tunneling
- Return Routability procedure
- Correspondent registration
- Returning home scenario

# 4 SIMULATION SETUP

INET Framework version 2.2 and xMIPv6 are used to implement this simulation.

## 4.1 NETWORK TOPOLOGY

The Proposed Network scenario is composed by Home Network, Foreign Network, Home Agent, Mobile Node, Correspondent Node, two access points, and core routers. Both home and foreign network each have one Access Point connected to access routers. Each access point has a range of approximately 150 meters. For wired connectivity we used Ethernet link with data-rate of 100 Mbps and delay of 0.1µS. And for wireless connectivity 802.11 is used. Each access points configured to be synchronized in different channels. For that channel control module is used. Following are some components used in this network:

- **FlatNetworkConfigurator6:** This is INET IPv6 implementation for configuring IPv6 addresses and routing tables.
- **Router6**: Router with IPv6 capability.
- **Home Agent:** IPv6 Router configured to operate as home agent in MIPv6 supporting environment.
- **CorrespondentNode6:** IPv6 Router which acts as correspondent node. It contains Binding Cache which gets updated with every Binding Update received.
- **Access Point:** A generic access point supporting multiple wireless radios and Ethernet ports. The mgmtType of wlan can be configured for different management types currently it can be: Ieee80211MgmtAPSimplified and Ieee80211MgmtAP. By default it is Ieee80211MgmtAP. The Simplified version does not support channel scanning, authentication and association. In this case, nodes must explicitly specify the hardware address of the wlan card they want to be associated with.
- **Channel Control:** Channel Control has exactly one instance in every network model that contains mobile or wireless nodes. This module gets informed about the location and movement of nodes, and determines which nodes are within communication or interference distance. This info is then used by the radio interfaces of nodes at transmissions.
- **WirelessHost6:** IPv6 compatible wireless host acting as mobile node with MIPv6 support. Models a host with one wireless (802.11) card in infrastructure mode, supports handovers and MIPv6 protocol. This module is basically a StandardHost with an Ieee80211NicSTA and MobileIPLayer6 added. It should be used in conjunction with Access Point.
- **Routing Table Recorder:** Record changes in routing table and interface table of all routers and hosts.

Following is the proposed network that was tested on OMNeT++ simulator on IPv4 and IPv6 environment.

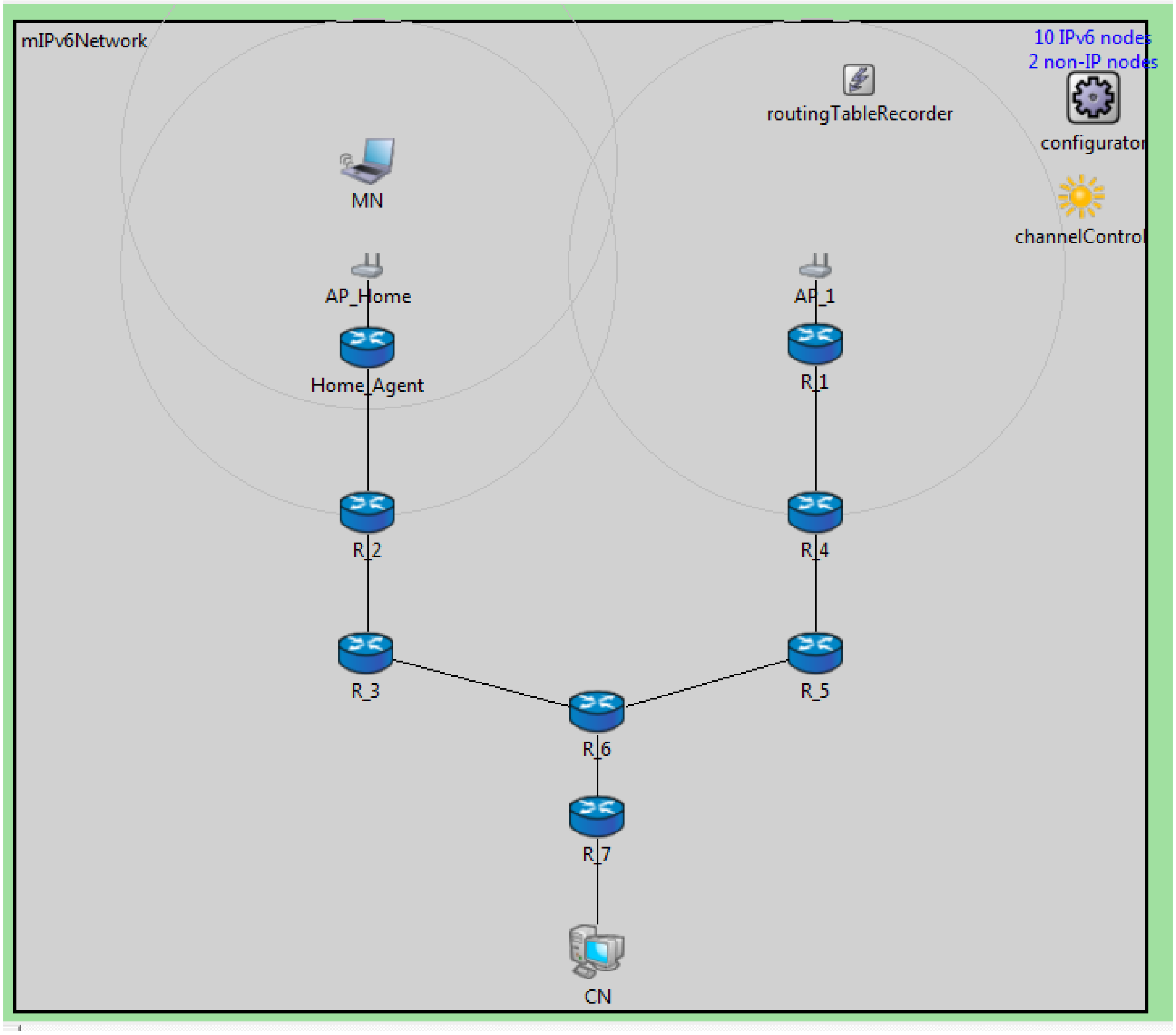

*Figure 4: Network Topology*

In this network core routers models Internet by adjusting link delays.

## 4.2 SIMULATION SCENARIO

In this section we discuss the simulation scenario and parameters we used to support/ run this simulation.

### 4.2.1 Parameters

| Simulation Model | Parameter | Value |
|---|---|---|
| Wireless (IEEE 802.11) | probeDelay<br>minChannelTime<br>maxChannelTime<br>authenticationTimeout<br>associationTimeout<br>transmitterPower<br>carrierfrequency<br>sensitivity<br>channeltoscan<br>numAuthSteps<br>framecapacity<br>becaonInterval<br>pMax<br>sat | 100ms<br>0.15s<br>0.3s<br>5s<br>5s<br>2.0mW<br>2.4GHz<br>-82dBm<br>1, 2<br>4<br>10<br>0.1s<br>2.0mW<br>-82dBm |
| Wired (Ethernet) | Delay<br>Datarate<br>queueType<br>promiscuous<br>mac.address<br>duplexMode<br>mtu | 0.1µs<br>100Mbps<br>DropTailQueue<br>False<br>auto<br>true<br>1500B |
| Mobility | mobilityType<br>acceleration<br>speed<br>updateInterval | Linear<br>0<br>5mps<br>500ms |
| MIPv6 | minIntervalBetweenRAs<br>maxIntervalBetweenRAs | 0.03s<br>0.07s |

*Table 1: Simulation Parameters*

Simulation run time=60s

Warm up period=10s

We will be using CN as UDP video server in network and MN as UDP video client. UDP video server is operating on port 3018. Video size is 1 MB. And server CN is sending packet at interval of 20 milliseconds. Each packet is of 1000 Bytes length.

First MN will request for video stream at 10 seconds, at that time MN will be in home network associating with AP_Home. To check route optimization MN need to communicate with CN when it is away from home network, so MN will request again for video streaming at 35 seconds. In our scenario, we deduce that after 34.7 seconds MN will associate with AP_1 instead of AP_Home.

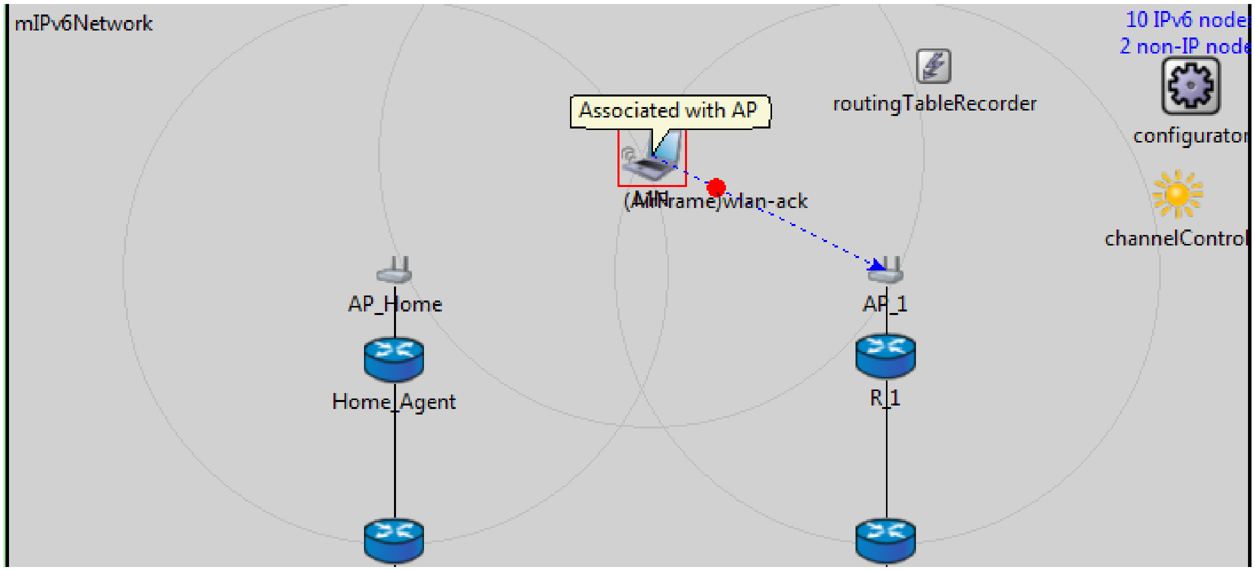

*Figure 5: MN in Foreign Network*

# 5 PERFORMANCE ANALYSIS

In this section we will study the results we acquired from our simulation in IPv6 environment.

## 5.1 END TO END DELAY

In this section we will first examine end to end delay between MN and CN when MN is in Home Network. Following table represent the results we got from the scalar files from our simulation.

| Module | Name | Value |
|---|---|---|
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:count | 1049.0 |
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:max | 0.002172742007 |
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:mean | 0.00074193685496187 |
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:min | 0.000469166874 |
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:sqrsum | 0.00058153567981069 |
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:stddev | 0.000062489224408514 |
| mIPv6Network.MN.udpApp[0] | endToEndDelay:histogram:sum | 0.778291760855 |

*Table 2: End to end delay in Home Network*

From this table we can infer that MN received 1049 video packets from CN when in home network. Maximum end to end delay is 2.17 milliseconds. Minimum end to end delay is 0.47 milliseconds. And total end to end delay is 0.7 seconds.

Now we will observe the end to end delay between MN and CN when MN is in foreign network. It is important because that way we can check if Mobile IPv6 is using Route Optimization technique to send packets from CN to MN or normal routing techniques. Following table represent the results we got from the scalar files from our simulation.

| Module | Name | Value |
|---|---|---|
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:count | 1049.0 |
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:max | 0.002197727004 |
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:mean | 0.00074019069982841 |
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:min | 0.000468882748 |
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:sqrsum | 0.00057831562034402 |
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:stddev | 0.000058504884134577 |
| mIPv6Network.MN.udpApp[1] | endToEndDelay:histogram:sum | 0. 77646004412 |

*Table 3 End to end delay in Foreign Network*

From this table we can infer that MN received 1049 video packets from CN when in foreign network. Maximum end to end delay is 2.2 milliseconds. Minimum end to end delay is 0.4 milliseconds. And total end to end delay is 0.7 seconds.

## 5.2 THROUGHPUT

The following figure shows the throughput (bytes/second) for CN, Home_Agent, R_1, R_2, R_3, R_5, R_6, and R_7.

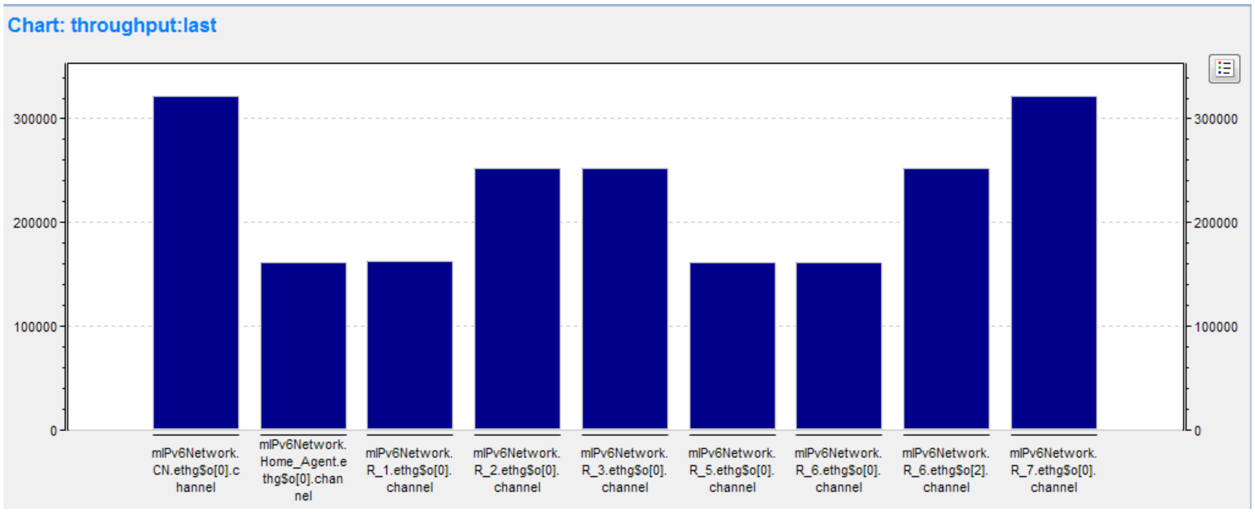

*Figure 6 Throughput*

# 6 CONCLUSION AND FUTURE WORK

In this project, performance analysis of Mobile IPv6 route optimization mechanism on real-time applications like video traffic in IPv6 environment was presented. So to understand route optimization clearly, it was necessary to have better insights on mobility protocols MIPv4 and MIPv6. From this project, it can be inferred that the major difference between MIPv4 and MIPv6 is route optimization which makes MIPv6 a better choice over MIPv4 to support mobility at network layer. The simulation was carried out on OMNeT++ simulator.

Handoff delay was calculated from simulation results by subtracting the association request time from the association confirm time and it was around 0.4 seconds. Here association time is time MN takes to associate with new access point in foreign network.

From the simulation test results, it was observed that the end to end delay for MN in both home and foreign network is almost the same. It shows that in foreign network MIPv6 route optimization technique was being used by CN to send video stream packets to MN. So observations clearly show that the end to end delay of the simulation is optimal for supporting real time applications.

In this project, video traffic was simulated for MIPv6. MN and CN were used as video client and server respectively. Core routers with 0.1µs link delay were used to simulate this network. In order to emulate more realistic behavior, MPLS could be used in core routers. However, current version of INET does not support IPv6 over MPLS.

# REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko (June 2004), Mobility Support in IPv6. RFC 3773.

[2] XiuJia Jin (April 2006), A survey on Network Architectures for Mobility.

[3] [Online] http://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol

[4] T. Narten, E. Nordmark, W. Simpson, H. Soliman (September 2007), Neighbor Discovery for IP version 6 (IPv6), RFC 4861.

[5] [Online] http://www.sixscape.com/

[6] [Online] http://packetlife.net/blog/2008/aug/28/ipv6-neighbor-discovery/

[7] OMNeT++, [Online] http://www.omnetpp.org/

[8] xMIPv6 Project, [Online] http://www.kn.e-technik.tu-dortmund.de/de/forschung/ausstattung/xmipv6.html

[9] Faqir Zarrar Yousaf, Christian Bauer, Christian Wietfeld, An Accurate and Extensible Mobile IPv6 Simulation model for OMNeT++.

[10] Athens University of Economics and Business (July 2012), Simulating mobility in a Realistic Networking Environment.

[11] S. Thomson, T. Narten, T. Jinmei (September 2007), IPv6 Stateless Address Autoconfiguration, RFC 4862.

[12] R. Draves (February 2003), Default Address Selection for Internet Protocol Version 6 (IPv6), RFC 3484.

[13] [Online] http://en.wikipedia.org/wiki/Mobile_IP

[14] Youn-Hen Han (February 2009), “Overview of IP Mobility Protocols”, Korea Uni. Of Technology.

[15] Timo Koskiahde (April 2002), “Security in Mobile IPv6”, Tampere University of Technology.

[16] Hong-Yon Lach, Christophe Janneteau, and Alexandru Petrescu, "Network Mobility in Beyond-3G Systems", IEEE Communications Magazine, July 2003. For Network Mobility.

[17] C. Ng., P. Thubert, H. Ohnishi, and E. Paik (February 2005), Taxonomy of route optimization models in the nemo context.

[18] P. Thubert and M. Molteni (February 2007), Ipv6 reverse routing header and its applications to mobile networks.

[19] [Online] http://www.tldp.org/HOWTO/html_single/Mobile-IPv6-HOWTO/

[20] [Online] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

[21] [Online] http://www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk/archives/200907.html